REMARKS

Claim Rejections - 35 USC §102

The examiner rejected claims 1, 10-15, 17, 26-31 under 35 USC §102(b) as anticipated by Blakley, III et al. (5,677,952).

Regarding claim 1, the examiner asserts that Blakley discloses a disk drive comprising a disk having a pristine area and authentication circuitry for authenticating a request received from an external entity to access the pristine area, a secret drive key, and decryption circuitry for decrypting encrypted data stored in the pristine area using the secrete drive key. The applicant respectfully disagrees.

Although Blakley discloses a disk drive in FIG. 3, Blakley does not disclose or suggest to implement an authentication facility within a disk drive as recited in the claim. In contrast, Blakley discloses to implement an authentication facility for accessing a disk drive within the operating system of the host computer. Referring to FIG. 3, col. 5, lines 28-31, Blakley discloses that the authentication facility (login utility 80) is implemented by the operating system running on the host computer. The rejection should therefore be withdrawn since Blakley does not disclose or suggest to implement an authentication facility within a disk drive.

Further, Blakley does not disclose or suggest a disk drive that comprises a secrete drive key for decrypting encrypted data stored on the disk. Referring again to FIG. 3, col. 5, lines 31-40, Blakley discloses that that generation of a decryption key (pseudorandom bit string) is implemented by the operating system running on the host computer. At col. 3, lines 40-45, Blakley states: "Preferably, the requisite secrete key is not present on the storage device; rather, it resides in memory when the machine (host computer) is in use". Therefore, Blakley teaches away from the invention recited in claim 1 by teaching that the decryption key resides in a memory of the host computer rather than within the disk drive. The rejection should therefore be withdrawn.

Still further, Blakley does not disclose or suggest a disk drive that comprises decryption circuitry for decrypting encrypted data stored on the disk. Referring again to FIG. 3, col. 5, lines 31-40, Blakley discloses a function 84 implemented in a device driver of the host computer's operating system for decrypting encrypted data stored on the disk drive. Since Blakley does not disclose to implement the decryption facility within the disk drive the rejection should be withdrawn.

Regarding claim 11, the examiner asserts that Blakley discloses a disk drive comprising encryption circuitry for encrypting plaintext data into encrypted data stored on the disk. However, at col. 5, lines 31-40, Blakley discloses a function 84 implemented in a device driver of the host computer's operating system for encrypting data stored on the disk drive. Since Blakley does not disclose to implement the encryption facility within the disk drive the rejection should be withdrawn.

Regarding claim 12, the examiner asserts that Blakley teaches a disk drive comprising a servo control system wherein the authentication circuitry enables the servo control system. The applicant respectfully disagrees.

Although the disk drive disclosed by Blakley would comprise a servo control system, nothing in Blakley discloses or suggests to implement an authentication facility within the disk drive for enabling the servo control system. The rejection should be withdrawn.

Regarding claims 13 and 14, the examiner asserts that Blakley teaches to write servo bursts to the disk in encrypted form and to decrypt the servo bursts in response to authentication circuitry. The applicant respectfully disagrees.

Blakley teaches to encrypt the user data stored in the sectors of the disk drive (col. 3, lines 50-55). Blakley does not disclose or suggest to encrypt servo bursts written in the

embedded servo sectors, let alone to encrypt the servo bursts using additive noise generated from a pseudo random sequence. The rejection should be withdrawn.

Regarding claims 15 and 31, the examiner asserts that Blakley teaches to decrypt encrypted data stored on the disk of a disk drive and to use the decrypted data to authenticate an access request received from an external entity. The applicant respectfully disagrees.

In col. 5, lines 51-53, Blakely discloses to store on the disk in the clear identification data used to authenticate a particular user. It is well known that the term "in the clear" means that the data is not stored in an encrypted form as recited in the claim. Further as described above, Blakely does not disclose or suggest to implement the authentication and decryption facilities and a secrete drive key within the disk drive. The rejection should be withdrawn.

Claim Rejections - 35 USC §103

The examiner rejected claims 9 and 25 under 35 USC §103(a) as unpatentable over Blakley in view of Nozawa et al (5,235,641). The applicant respectfully disagrees.

Although Nozawa teaches to store encrypted key data on a disk of a disk drive, Nozawa teaches to decrypt the encrypted key data at the upper rank apparatus (the host computer). See FIG. 1 element 11 and col. 6, lines 36-55. The rejection should therefore be withdrawn.

The examiner rejected claims 2-8, 18-24 under 35 USC §103(a) as unpatentable over Blakley in view of Scott et al (EP 816967 A2). The applicant respectfully disagrees.

Regarding claim 2, the examiner asserts that Scott teaches to store encrypted authentication data on a disk drive. However, Scott teaches to decrypt the authentication

data and to perform the authentication process in the host computer rather than in the disk drive as recited in the claims. See col. 5, lines 11-12. The rejection should therefore be withdrawn.

The rejection of the remaining claims should be withdrawn for the reasons set forth above.

CONCLUSION

The above amendments to the claims do not add new matter or raise new issues; the applicant respectfully requests the amendments be entered. In view of the foregoing remarks, the rejections should be withdrawn. In particular, the relied upon prior art does not disclose or suggest to implement within a disk drive an authentication facility, a secret drive key, and a decryption facility using the secrete drive key. The examiner is encouraged to contact the undersigned over the telephone in order to resolve any remaining issues that may prevent the immediate allowance of the present application.

Respectfully submitted,

Date: 4/22/04 By: _____

Howard H. Sheerin
Reg. No. 37,938
Tel. No. (303) 765-1689

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

4/22/04 Howard H. Sheerin
(Date) (Print Name)

_____
(Signature)